Učební texty k přednášce ALGEBRAICKÉ STRUKTURY
Michal Marvan, Matematický ústav
Slezská univerzita v Opavě

2. Homomorfismy

Definice. Buďte $(A, (\alpha_i)_{i\in I})$ a $(B, (\beta_i)_{i\in I})$ dvě algebry jedné a téže signatury (I, n). Zobrazení $f : A \to B$ se nazývá *homomorfismus*, jestliže

(1) Pro každé $i \in I$ takové, že $n_i = 0$ platí

$$f(\alpha_i) = \beta_i.$$

(2) Pro každé $i \in I$ takové, že $n_i > 0$ platí

$$f(\alpha_i(a_1, \dots, a_{n_i})) = \beta_i(f(a_1), \dots, f(a_{n_i})) \quad \text{pro všechna } a_1, \dots, a_{n_i} \in A.$$

Podmínka (1) říká, že homomorfismy zobrazují nulární operace na nulární operace. Podmínka (2) znamená, že homomorfismy jsou *záměnné* s operacemi kladné arity: obraz výsledku operace = výsledek operace na obrazech.

Definice. Bijektivní homomorfismus se nazývá *izomorfismus*.

Příklad. Uvažujme o aditivní grupě $(\mathbf{R}, +, 0, -)$ a multiplikativní grupě $(\mathbf{R}^+, \cdot, 1, ^{-1})$, kde $\mathbf{R}^+$ je množina všech kladných reálných čísel (snadno se ověří, že je to grupa). Ukažme, že mezi $\mathbf{R}$ a $\mathbf{R}^+$ existují netriviální homomorfismy.

Vskutku, zobrazení $f : \mathbf{R} \to \mathbf{R}^+$ je homomorfismem, platí-li $f(x+y) = f(x)\cdot f(y)$, $f(0) = 1$, $f(-x) = f(x)^{-1}$. Těmto požadavkům lze vyhovět například tak, že položíme $f(x) = a^x$, kde a je libovolné kladné reálné číslo. Pro $a \neq 1$ je takové zobrazení navíc bijektivní, a tedy izomorfismus.

Podobně, zobrazení $g : \mathbf{R}^+ \to \mathbf{R}$ je homomorfismem, platí-li $g(x\cdot y) = g(x)+g(y)$, $g(1) = 0$, $g(x^{-1}) = -g(x)$. Těmto požadavkům lze vyhovět například tak, že položíme $g(x) = \log_a x$, kde a je libovolné kladné reálné číslo. Opět, pro $a \neq 1$ je takové zobrazení navíc bijektivní, a tedy izomorfismus.

Logaritmus jako nástroj převádějící násobení na sčítání tak dostává nový smysl: jedná se vlastně o izomorfismus aditivní a multiplikativní grupy.

Příklad. Homomorfismy vektorových prostorů $(U, +, 0, -, P) \to (V, +, 0, -, P)$ jsou právě P-lineární zobrazení. (Dokažte.)

Tvrzení. *Buďte $(A, (\alpha_i))$, $(B, (\beta_i))$, $(C, (\gamma_i))$ tři algebry signatury (I, n), buďte $f : A \to B$, $g : B \to C$ zobrazení. Pak*

(i) *Jsou-li f, g homomorfismy, pak je i $g \circ f$ homomorfismus.*
(ii) *Identické zobrazení $\mathrm{id}_A : A \to A$ je vždy izomorfismus.*
(iii) *Je-li f izomorfismus, pak i $f^{-1} : B \to A$ je izomorfismus.*
(iv) *Jsou-li f, g izomorfismy, pak je i $g \circ f$ izomorfismus.*

Důkaz. Důkaz podáme pro operace arity $n > 0$. Případ $n = 0$ zůstává jako snadné cvičení.

(i) Buď $i \in I$ takové, že $n_i > 0$. Podle předpokladu jsou f, g homomorfismy, a proto pro libovolná $a_1, \dots, a_{n_i} \in A$, $b_1, \dots, b_{n_i} \in B$ platí

$$f(\alpha_i(a_1, \dots, a_{n_i})) = \beta_i(f(a_1), \dots, f(a_{n_i})) \tag{1}$$

$$g(\beta_i(b_1, \dots, b_{n_i})) = \gamma_i(g(b_1), \dots, g(b_{n_i})). \tag{2}$$

Pak ovšem pro libovolná $a_1, \ldots, a_{n_i} \in A$ máme

$$(g \circ f)(\alpha_i(a_1, \ldots, a_{n_i})) = g(f(\alpha_i(a_1, \ldots, a_{n_i}))) \overset{(1)}{=} g(\beta_i(f(a_1), \ldots, f(a_{n_i})))$$
$$\overset{(2)}{=} \gamma_i(g(f(a_1)), \ldots, f(a_{n_i}))) = \gamma_i((g \circ f)(a_1), \ldots, (g \circ f)(a_{n_i})).$$

Vidíme, že $g \circ f$ je homomorfismus.

(ii) Triviální.

(iii) Nechť opět $n_i > 0$. Buďte $b_1, \ldots, b_{n_i} \in B$ libovolná. Požadujeme rovnost

$$\alpha_i(f^{-1}(b_1), \ldots, f^{-1}(b_{n_i})) = f^{-1}(\beta_i(b_1, \ldots, b_{n_i})).$$

Snadno však spočítáme, že

$$f(\alpha_i(f^{-1}(b_1), \ldots, f^{-1}(b_{n_i})) \overset{(1)}{=} \beta_i(f(f^{-1}(b_1)), \ldots, f(f^{-1}(b_{n_i})))$$
$$= \beta_i(b_1, \ldots, b_{n_i}).$$

Aplikujeme-li na obě strany poslední rovnosti f^{-1}, obdržíme požadovanou rovnost.

(iv) Plyne z (i) a z toho, že složení bijekcí je bijekce.

Existuje-li mezi dvěma algebrami A, B alespoň jeden izomorfismus, říkáme, že jsou *izomorfní* a zapisujeme $A \cong B$.

Důsledek. *Pro libovolné tři algebry A, B, C jedné a téže signatury platí:*

1. $A \cong A$.
2. *Je-li* $A \cong B$, *pak také* $B \cong A$.
3. *Je-li* $A \cong B$, $B \cong C$, *pak také* $A \cong C$.

Je-li $f : A \to B$ bijekce mezi množinami, často se hodí, že se množiny A a B mohou ztotožnit (prvek $a \in A$ se ztotožní s prvkem $f(a) \in B$). Je-li $f : A \to B$ izomorfismus mezi algebrami, pak se při takovém ztotožnění zachovají i výsledky operací — dvě izomorfní algebry jsou tak "v podstatě stejné."

Příklad. Uvažujme o aditivní grupě $(\mathbf{Q}, +, 0, -)$ a multiplikativní grupě $(\mathbf{Q}^+, \cdot, 1, ^{-1})$, kde $\mathbf{Q}$ je množina všech racionálních čísel a $\mathbf{Q}^+$ je množina všech kladných racionálních čísel (přesvědčte se, že jde o grupy). Ukažme, že $\mathbf{Q}$ a $\mathbf{Q}^+$ *nejsou izomorfní* (porovnejte s výsledkem předchozího příkladu). Využijeme přitom známého faktu, že rovnice $z^2 = 2$ nemá řešení v racionálních číslech.

Připusťme, že zobrazení $f : \mathbf{Q} \to \mathbf{Q}^+$ je izomorfismus, tj. že je bijektivní a pro libovolná $x, y \in \mathbf{Q}$ platí mimo jiné $f(x + y) = f(x) \cdot f(y)$. Položme $y = f^{-1}(2)$, nechť $x = \frac{1}{2}y$. Pak pro $z := f(x) \in \mathbf{Q}$ dostáváme

$$z^2 = f(x) \cdot f(x) = f(x + x) = f(y) = 2.$$

Vidíme, že $z := f(x)$ je racionální číslo a zároveň kořen rovnice $z^2 = 2$, což je spor.

Cvičení. Ukažte, že tvrzení $(*)$ "Pro každé $a \in A$ existuje $z \in A$ takové, že $z \cdot z = a$" současně platí nebo současně neplatí ve všech izomorfních grupách. Vyjmenujte všechny Vám známé grupy, ve kterých tvrzení $(*)$ platí.